(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
1 septembre 2005 (01.09.2005)

PCT

(10) Numéro de publication internationale
WO 2005/081525 A1

(51) Classification internationale des brevets[7] :
H04N 7/167, 5/00, 7/16

(21) Numéro de la demande internationale :
PCT/FR2005/050101

(22) Date de dépôt international :
17 février 2005 (17.02.2005)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0450323 20 février 2004 (20.02.2004) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **VIACCESS** [FR/FR]; Les Collines de l'Arche - Tour Opéra C, F-92057 PARIS LA DEFENSE CEDEX (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **BEUN, Frédéric** [FR/FR]; 30, avenue Guy de Maupassant, F-78400 CHATOU (FR). **BOUDIER, Laurence** [FR/FR]; 30, avenue Guy de Maupassant, F-78400 CHATOU (FR). **ROQUE, Pierre** [FR/FR]; 30, rue Sedaine, F-75011 PARIS (FR). **TRONEL, Bruno** [FR/FR]; 9 rue de l'Oasis, F-92800 PUTEAUX (FR).

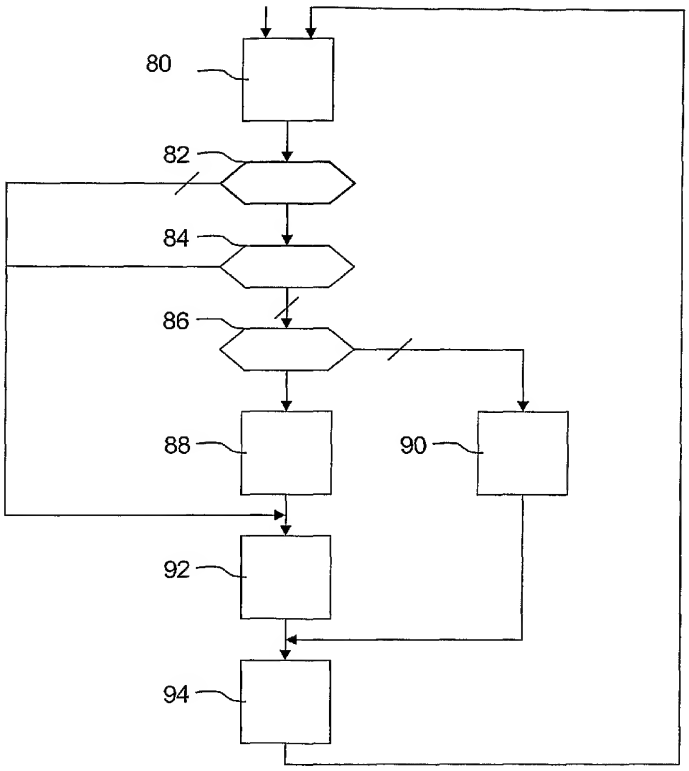
(74) Mandataire : **POULIN, Gérard**; BREVALEX, 3, rue du Docteur Lancereaux, F-75008 PARIS (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG,

[Suite sur la page suivante]

(54) Title: METHOD FOR MATCHING A RECEIVER TERMINAL TO A NUMBER OF ACCESS CONTROL CARDS

(54) Titre : PROCEDE D'APPARIEMENT D'UN TERMINAL RECEPTEUR AVEC UNE PLURALITE DE CARTES DE CONTROLE D'ACCES



(57) Abstract: The invention relates to a method for matching a receiver unit (2) to a number of security modules (6, 8), each having a unique identifier. According to the invention, said method comprises the following steps: connection of a security module (6, 8) to the receiver unit (2), storage on the fly of the unique identifier for the connected security module (6, 8) in the receiver unit (2).

(57) Abrégé : L'invention concerne un procédé d'appariement d'un équipement récepteur (2) avec une pluralité de modules de sécurité (6, 8) ayant chacun un identifiant unique. Le procédé selon l'invention comporte les étapes suivantes : - connecter un module de sécurité (6, 8) à l'équipement récepteur (2), - mémoriser à la volée dans l'équipement récepteur (2) l'identifiant unique du module de sécurité (6, 8) connecté.

WO 2005/081525 A1

KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* **:** ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

PROCEDE D'APPARIEMENT D'UN TERMINAL RECEPTEUR AVEC UNE PLURALITE DE CARTES DE CONTROLE D'ACCES

DESCRIPTION

DOMAINE TECHNIQUE

L'invention se situe dans le domaine de la sécurisation de données numériques diffusées et des équipements récepteurs destinés à recevoir ces données dans un réseau de distribution de données et/ou services et se rapporte plus spécifiquement à un procédé d'appariement d'un équipement récepteur de données numériques avec une pluralité de modules externes de sécurité ayant chacun un identifiant unique.

ÉTAT DE LA TECHNIQUE ANTÉRIEURE

De plus en plus d'opérateurs offrent des données et services en ligne accessibles au moyen de terminaux munis de processeurs de sécurité. Généralement, les données et services distribués sont embrouillés à l'émission par des clés secrètes et désembrouillés à la réception par les mêmes clés secrètes préalablement mises à la disposition de l'abonné.

Outre les techniques classiques de contrôle d'accès basées sur l'embrouillage à l'émission et le désembrouillage à la réception des données distribuées, les opérateurs proposent des techniques basées sur l'appariement du terminal de réception avec un processeur de sécurité pour éviter que les données et services distribués ne soient accessibles à des utilisateurs muni d'un terminal volé ou d'un processeur

de sécurité piraté tel que par exemple une carte à puce falsifiée.

Le document WO 99/57901 décrit un mécanisme d'appariement entre un récepteur et un module de sécurité basé, d'une part, sur le chiffrement et le déchiffrement des informations échangées entre le récepteur et le module de sécurité par une clé unique stockée dans le récepteur ou dans le module de sécurité, et d'autre part, sur la présence d'un numéro de récepteur dans le module de sécurité.

Un inconvénient de cette technique provient du fait que l'association entre un récepteur et un module de sécurité qui lui est apparié est établie a priori, et qu'elle ne permet pas à l'opérateur de gérer efficacement son parc d'équipements récepteurs afin d'empêcher le détournement de cet équipement pour des utilisations frauduleuses.

Un but du procédé d'appariement selon l'invention est de permettre à chaque opérateur de limiter les utilisations de son parc de matériel de réception en configurant et en contrôlant dynamiquement l'appariement de l'équipement récepteur et des modules externes de sécurité destinés à coopérer avec cet équipement.

EXPOSÉ DE L'INVENTION

L'invention préconise un procédé d'appariement d'un équipement récepteur de données numériques avec une pluralité de modules externes de sécurité ayant chacun un identifiant unique.

Le procédé selon l'invention comporte les étapes suivantes :

- connecter un module externe de sécurité à l'équipement récepteur,
- mémoriser à la volée dans l'équipement récepteur l'identifiant unique du module de sécurité connecté.

Ce procédé comporte une phase de contrôle consistant à vérifier, à chaque connexion ultérieure d'un module externe de sécurité à l'équipement récepteur, si l'identifiant dudit module est mémorisé dans cet équipement récepteur.

A cet effet, le procédé selon l'invention comporte en outre une étape consistant à transmettre à l'équipement récepteur une signalisation comportant au moins un message de gestion de la mémorisation de l'identifiant du module externe de sécurité et/ou un message de gestion de la phase de contrôle.

Ladite signalisation comporte au moins une des consignes suivantes :

- autoriser la mémorisation,
- interdire la mémorisation,
- effacer les identifiants déjà mémorisés dans l'équipement récepteur,
- activer ou désactiver la phase de contrôle.

Dans une première variante de mise en œuvre du procédé, la signalisation comporte le nombre maximal d'identifiants dont la mémorisation est autorisée.

Dans une deuxième variante de mise en œuvre du procédé, ladite signalisation comporte une consigne

de reconfiguration par laquelle on transmet à l'équipement récepteur une liste mise à jour des identifiants des modules externes de sécurité appariés avec ledit équipement récepteur.

Ladite liste est transmise soit directement à l'équipement récepteur, soit via un module externe de sécurité connecté audit équipement récepteur.

Préférentiellement, ladite phase de contrôle comporte une procédure consistant à perturber le traitement des données si l'identifiant du module externe de sécurité connecté n'est pas préalablement mémorisé dans l'équipement récepteur.

Le procédé selon l'invention s'applique lorsque les données sont distribuées en clair et également lorsque ces données sont distribuées sous forme embrouillée par un mot de contrôle chiffré. Dans ce dernier cas, chaque module externe de sécurité comporte des droits d'accès auxdites données et un algorithme de déchiffrement dudit mot de contrôle pour désembrouiller les données.

La signalisation de contrôle est transmise dans un message EMM (Entitlement Management Message, en anglais) spécifique à un module externe de sécurité associé à cet équipement récepteur ou dans un message EMM spécifique à cet équipement récepteur, et pour un équipement récepteur donné, la liste mise à jour des identifiants des modules externes de sécurité appariés avec cet équipement récepteur est également transmise dans un message EMM spécifique à un module de sécurité associé à cet équipement récepteur.

Alternativement, ladite signalisation est transmise dans un flux privé à un groupe d'équipements récepteurs, et la liste mise à jour des identifiants des modules externes est également transmise dans un flux privé à chaque équipement récepteur. Dans ce dernier cas, ledit flux privé est traité par un logiciel dédié exécutable dans chaque équipement récepteur en fonction de l'identifiant du module externe de sécurité qui lui est associé.

Dans une autre variante, la signalisation est transmise à un groupe d'équipements récepteurs dans un message EMM spécifique à un groupe de modules externes de sécurité associés auxdits équipements récepteurs ou dans un message EMM spécifique audit groupe d'équipements récepteurs, et pour un groupe d'équipements récepteurs donné, la liste mise à jour des identifiants des modules externes est transmise dans un message EMM spécifique à un groupe de modules externes de sécurité associés auxdits équipements récepteurs.

Par ailleurs, pour un groupe d'équipements récepteurs donné, la signalisation de contrôle et la liste mise à jour peuvent également être transmises à un groupe d'équipements dans un flux privé.

Dans ce cas, ledit flux privé est traité par un logiciel dédié exécutable dans chaque équipement récepteur en fonction de l'identifiant du module externe de sécurité qui lui est associé.

Lorsque la transmission de la signalisation et des listes mises à jour est effectuée par des EMM, le procédé comporte un mécanisme destiné à empêcher

l'utilisation d'un EMM transmis à un même module de sécurité dans deux équipements récepteurs distincts.

Les EMM spécifiques à un module de sécurité ou à un équipement récepteur présentent le format suivant :

```
EMM-U_section() {
table_id = 0x88                          8 bits
section_syntax_indicator = 0             1 bit
DVB_reserved                             1 bit
ISO_reserved                             2 bits
EMM-U_section_length                     12 bits
unique_adress_field                      40 bits
for (i=0; i<N; i++) {
    EMM_data_byte                        8 bits
    }
}
```

Les EMM spécifiques à tous les modules externes de sécurité ou à tous les équipements récepteurs présentent le format suivant :

```
EMM-G_section() {
table_id = 0x8A ou 0x8B                  8 bits
section_syntax_indicator = 0             1 bit
DVB_reserved                             1 bit
ISO_reserved                             2 bits
EMM-G_section_length                     12 bits
for (i=0; i<N; i++) {
    EMM_data_byte                        8 bits
    }
}
```

Les EMM spécifiques à un sous-groupe de modules externes de sécurité ou à un sous-groupe d'équipements récepteurs présentent le format suivant :

```
EMM-S_section() {
table_id = 0x8E                          8 bits
section_syntax_indicator = 0             1 bit
DVB_reserved                             1 bit
ISO_reserved                             2 bits
EMM-S_section_length                     12 bits
shared_address_field                     24 bits
reserved                                 6 bits
data_format                              1 bit
ADF_scrambling_flag                      1 bit
for (i=0; i<N; i++) {
    EMM_data_byte                        8 bits
    }
}
```

Selon une caractéristique supplémentaire, les identifiants de modules de sécurité sont groupés dans une liste chiffrée.

Le procédé peut être utilisé dans une première architecture, dans laquelle l'équipement récepteur comporte un décodeur et le module de sécurité comporte une carte de contrôle d'accès dans laquelle sont mémorisées des informations relatives aux droits d'accès d'un abonné à des données numériques distribuées par un opérateur.

Dans cette architecture, l'appariement est effectué entre le décodeur et la carte de contrôle d'accès.

Le procédé peut être utilisé dans une deuxième architecture dans laquelle l'équipement récepteur comporte un décodeur et le module de sécurité comporte une interface de sécurité amovible munie d'une mémoire non volatile et destinée à coopérer, d'une

part, avec le décodeur, et d'autre part, avec une pluralité de cartes de contrôle d'accès conditionnel pour gérer l'accès à des données numériques distribuées par un opérateur.

Dans cette architecture, l'appariement est effectué entre ledit décodeur et ladite interface de sécurité amovible.

Le procédé peut être utilisé dans une troisième architecture dans laquelle l'équipement récepteur comporte un décodeur muni d'une interface de sécurité amovible ayant une mémoire non volatile et destinée à coopérer, d'une part, avec ledit décodeur, et d'autre part, avec une pluralité de cartes de contrôle d'accès conditionnel.

Dans cette architecture, l'appariement est réalisé entre ladite interface de sécurité amovible et lesdites cartes de contrôle d'accès.

Dans une application particulière du procédé selon l'invention, les données sont des programmes audiovisuels.

Le procédé selon l'invention est mis en œuvre dans un système comportant une pluralité d'équipements récepteurs connectés à un réseau de diffusion de données et/ou services, chaque équipement récepteur étant susceptible d'être apparié avec une pluralité de modules externes de sécurité, ce système comportant également une plateforme de gestion commerciale communiquant avec lesdits équipements récepteurs et avec lesdits modules externes de sécurité. Ce système comporte en outre :

- un premier module agencé dans ladite plate-forme de gestion commerciale et destiné à générer des requêtes d'appariement,

- et un deuxième module agencé dans lesdits équipements récepteurs et destiné à traiter lesdites requêtes pour préparer une configuration de l'appariement et pour contrôler cet appariement.

L'invention concerne également un équipement récepteur susceptible d'être apparié avec une pluralité de modules externes de sécurité pour gérer l'accès à des données numériques distribuées par un opérateur.

Selon l'invention, cet équipement comporte des moyens pour mémoriser à la volée l'identifiant de chaque module externe de sécurité qui lui est connecté.

Dans un premier mode de réalisation, l'équipement récepteur comporte un décodeur et le module externe de sécurité est une carte de contrôle d'accès comportant des informations relatives aux droits d'accès d'un abonné auxdites données numériques, l'appariement étant effectué entre ledit décodeur et ladite carte.

Dans un deuxième mode de réalisation, l'équipement comporte un décodeur et le module externe de sécurité est une interface de sécurité amovible munie d'une mémoire non volatile et destinée à coopérer, d'une part, avec ledit décodeur, et d'autre part, avec une pluralité de cartes de contrôle d'accès conditionnel, pour gérer l'accès auxdites données numériques, l'appariement étant effectué entre ledit décodeur et ladite interface de sécurité amovible.

Dans un troisième mode de réalisation, l'équipement comporte un décodeur muni d'une interface de sécurité amovible ayant une mémoire non volatile et destinée à coopérer, d'une part, avec ledit décodeur, et d'autre part, avec une pluralité de cartes de contrôle d'accès conditionnel et l'appariement est réalisé entre ladite interface de sécurité amovible et lesdites cartes de contrôle d'accès.

L'invention concerne également un décodeur susceptible de coopérer avec une pluralité de modules externes de sécurité pour gérer l'accès à des programmes audiovisuels distribués par un opérateur, chaque module externe de sécurité ayant un identifiant unique et comportant au moins un algorithme de traitement de données.

Le décodeur selon l'invention comporte des moyens pour mémoriser à la volée l'identifiant de chaque module externe de sécurité qui lui est connecté.

Dans un premier mode de réalisation, lesdits modules externes de sécurité sont des cartes de contrôle d'accès dans lesquelles sont mémorisées des informations relatives aux droits d'accès d'un abonné à des données numériques distribuées par un opérateur.

Dans un deuxième mode de réalisation, lesdits modules externes de sécurité sont des interfaces de sécurité amovibles comportant une mémoire non volatile et destinées à coopérer, d'une part, avec le décodeur, et d'autre part, avec une pluralité de cartes de contrôle d'accès conditionnel pour gérer l'accès à des données numériques distribuées par un opérateur.

L'invention concerne également une interface de sécurité amovible comportant une mémoire non volatile et destinée à coopérer, d'une part, avec un équipement récepteur, et d'autre part, avec une pluralité de cartes de contrôle d'accès conditionnel, pour gérer l'accès à des données numériques distribuées par un opérateur, chaque carte ayant un identifiant unique et comportant des informations relatives aux droits d'accès d'un abonné auxdites données numériques.

L'interface selon l'invention comporte des moyens pour enregistrer à la volée l'identifiant de chaque carte de contrôle d'accès dans ladite mémoire non volatile.

Dans une première variante, cette interface est une carte PCMCIA (pour Personal Computer Memory Card International Association) comportant un logiciel de désembrouillage de données numériques.

Dans une deuxième variante, cette interface est un module logiciel qui peut être exécuté soit dans l'équipement récepteur soit dans le module externe de sécurité.

L'invention concerne en outre un programme d'ordinateur exécutable dans un équipement récepteur susceptible de coopérer avec une pluralité de modules externes de sécurité ayant chacun un identifiant unique et dans lesquels sont stockées des informations relatives aux droits d'accès d'un abonné à des données numériques distribuées par un opérateur.

Ce programme d'ordinateur comporte des instructions pour mémoriser à la volée l'identifiant de chaque module externe de sécurité connecté audit

équipement récepteur et des instructions destinées à générer localement des paramètres de contrôle de l'appariement de l'équipement récepteur avec un module externe de sécurité en fonction d'une signalisation transmise audit équipement récepteur par l'opérateur.

Ce Programme d'ordinateur comporte en outre des instructions destinées à vérifier, à chaque utilisation ultérieure d'un module externe de sécurité avec l'équipement récepteur, si l'identifiant dudit module externe de sécurité est mémorisé dans l'équipement récepteur.

BRÈVE DESCRIPTION DES DESSINS

D'autres caractéristiques et avantages de l'invention ressortiront de la description qui va suivre, prise à titre d'exemple non limitatif en référence aux figures annexées dans lesquelles :

- la figure 1 représente une première architecture pour la mise en œuvre de l'appariement selon l'invention,
- la figure 2 représente une deuxième architecture pour la mise en œuvre de l'appariement selon l'invention,
- la figure 3 représente une troisième architecture pour la mise en œuvre de l'appariement selon l'invention,
- la figure 4 représente la structure des messages EMM de configuration et d'utilisation des fonctionnalités d'appariement selon l'invention
- la figure 5 représente un diagramme d'état de la fonction d'appariement selon l'invention,

- la figure 6 représente un organigramme illustrant un mode particulier de mise en œuvre de l'appariement selon l'invention.

EXPOSÉ DÉTAILLÉ DE MODES DE RÉALISATION PARTICULIERS

L'invention va maintenant être décrite dans le cadre d'une application dans laquelle un opérateur diffusant des programmes audiovisuels met en œuvre le procédé selon l'invention pour limiter l'utilisation de son parc d'équipements récepteurs à ses propres abonnés.

Le procédé peut être mis en œuvre dans trois architectures distinctes illustrées respectivement par les figures 1, 2 et 3. Les éléments identiques dans ces trois architectures seront désignés par des références identiques.

La gestion de l'appariement est réalisée à partir d'une plateforme commerciale 1 contrôlée par l'opérateur et communiquant avec l'équipement récepteur installé chez l'abonné.

Dans la première architecture, illustrée par la figure 1, l'équipement récepteur comporte un décodeur 2 dans lequel est installé un logiciel de contrôle d'accès 4, et le module externe de sécurité est une carte de contrôle d'accès 6 comportant des informations relatives aux droits d'accès d'un abonné aux programmes audiovisuels diffusés. Dans ce cas, l'appariement est effectué entre le décodeur 2 et ladite carte 6.

Dans la deuxième architecture illustrée par la figure 2, l'équipement récepteur comporte un

décodeur 2, non dédié au contrôle d'accès, et le module externe de sécurité est une interface de sécurité amovible 8 munie d'une mémoire non volatile et dans laquelle est installé le logiciel de contrôle d'accès 4. Cette interface 8 coopère, d'une part, avec ledit décodeur 2, et d'autre part, avec une carte 6 parmi une pluralité de cartes de contrôle d'accès conditionnel, pour gérer l'accès auxdits programmes audiovisuels.

Dans cette architecture, l'appariement est réalisé entre ladite interface de sécurité amovible 8 et ladite carte de contrôle d'accès 6.

Dans la troisième architecture, illustrée par la figure 3, l'équipement récepteur comporte un décodeur 2 dans lequel est installé un logiciel de contrôle d'accès 4, ce décodeur 2 est connecté à une interface de sécurité amovible 8 ayant une mémoire non volatile qui coopère avec une carte 6 parmi une pluralité de cartes de contrôle d'accès conditionnel.

Dans ce cas, l'appariement est effectué entre le décodeur 2 et l'interface de sécurité amovible 8.

La configuration et l'utilisation par l'opérateur de l'appariement résulte de commandes émises par la plateforme de gestion commerciale 1.

La description qui suit concerne la mise en oeuvre de l'invention dans le cas d'appariement d'un décodeur 2 avec une carte 6. Les étapes mises en œuvre s'appliquent aux trois architectures décrites ci-dessus.

A la sortie d'usine d'un décodeur 2, comme après un téléchargement du logiciel de contrôle d'accès

4 dans ce décodeur, tous les traitements de l'appariement sont inactifs. En particulier :

- aucun identifiant de carte n'est mémorisé dans le décodeur 2,
- le nombre maximal d'identifiants de cartes mémorisables n'est pas initialisé,
- la mémorisation par le décodeur 2 de l'identifiant d'une carte 6 n'est pas active,
- le contrôle par le décodeur 2 de l'identifiant d'une carte 6 n'est pas actif.

Lorsqu'une carte valide est insérée dans le lecteur de carte prévu à cet effet dans le décodeur 2, l'appariement entre cette carte et le décodeur 2 peut alors être configuré par une requête de l'opérateur sur la plateforme de gestion 1 qui émet vers le décodeur 2 un message de gestion EMM dédié à l'appariement. Ce message de gestion EMM est adressé directement au décodeur 2 ou indirectement via la carte 6. Ce message de gestion EMM permet de réaliser les tâches suivantes :

- activer dans le décodeur 2 la fonction d'appariement ; dans ce cas le décodeur 2 vérifie si l'identifiant de la carte 6 fait partie des identifiants qu'il a mémorisés. Si ce n'est pas le cas, et si le nombre maximal d'identifiants de cartes mémorisables n'est pas atteint, le décodeur mémorise l'identifiant de cette carte.,
- désactiver dans le décodeur la fonction d'appariement. Dans ce cas le décodeur ne contrôle pas et ne mémorise pas l'identifiant de la carte 6,

- effacer les identifiants de cartes déjà mémorisés dans le décodeur.

- définir le nombre maximal d'identifiants de cartes mémorisables par le décodeur.

En outre l'opérateur peut émettre via la plateforme 1, un message EMM contenant une liste imposée des identifiants de cartes 6 appariées à un décodeur 2. Un tel message est adressé au décodeur 2 indirectement via la carte 6.

ADRESSAGE DES MESSAGES EMM

Les messages EMM permettant la configuration et l'utilisation des fonctionnalités liées à l'appariement selon le procédé de l'invention sont émis dans une voie EMM d'un multiplex numérique tel que défini par le standard MPEG2/Système et les standards DVB/ETSI.

Cette voie peut diffuser des EMM référençant une adresse de carte(s) permettant de les destiner :

- au décodeur dans lequel est insérée une carte particulière,

- aux décodeurs dans lesquels sont insérées les cartes d'un groupe particulier,

- aux décodeurs dans lesquels sont insérées toutes les cartes.

Ces EMM destinés aux décodeurs « via la carte » sont utilisés notamment quand les décodeurs ne disposent pas d'adresse.

Cette voie peut diffuser également des EMM référençant une adresse de décodeur(s) permettant de les destiner directement :

- à un décodeur particulier,
- à un groupe particulier de décodeurs,
- à tous les décodeurs ;

Les EMM directement destinés à tous les décodeurs sont utilisables également quand les décodeurs ne disposent pas d'adresse.

Les messages destinés à un décodeur désigné par une carte particulière ou directement à un décodeur particulier sont des EMM-U présentant la structure suivante :

```
EMM-U_section() {
table_id = 0x88                    8 bits
section_syntax_indicator = 0       1 bit
DVB_reserved                       1 bit
ISO_reserved                       2 bits
EMM-U_section_length               12 bits
unique_adress_field                40 bits
for (i=0; i<N; i++) {
    EMM_data_byte                  8 bits
    }
}
```

Le paramètre unique_adress_field est l'adresse unique d'une carte dans un EMM-U carte ou l'adresse unique d'un décodeur dans un EMM-U décodeur

Les messages destinés à des décodeurs désignés par un groupe particulier de cartes ou directement à un groupe particulier de décodeurs sont des EMM-S présentant la structure suivante :

EMM-S_section() {	
table_id = 0x8E	8 bits
section_syntax_indicator = 0	1 bit
DVB_reserved	1 bit
ISO_reserved	2 bits
EMM-S_section_length	12 bits
shared_address_field	24 bits
reserved	6 bits
data_format	1 bit
ADF_scrambling_flag	1 bit
for (i=0; i<N; i++) {	
EMM_data_byte	8 bits
}	
}	

Le paramètre shared_adress_field est l'adresse du groupe de cartes dans un EMM-S carte ou l'adresse du groupe de décodeurs dans un EMM-S décodeur. Un décodeur d'un groupe ou une carte d'un groupe est concerné(e) par le message si en outre il (elle) est explicitement désigné(e) dans un champ ADF contenu dans EMM_data_byte et pouvant être chiffré selon l'information ADF_scrambling_flag.

Les messages destinés aux décodeurs désignés par toutes les cartes ou directement à tous les décodeurs sont des EMM-G présentant la structure suivante :

```
EMM-G_section() {
table_id = 0x8A ou 0x8B          8 bits
section_syntax_indicator = 0     1 bit
DVB_reserved                     1 bit
ISO_reserved                     2 bits
EMM-G_section_length             12 bits
for (i=0; i<N; i++) {
    EMM_data_byte                8 bits
    }
}
```

CONTENU DES MESSAGES EMM

La figure 4 illustre schématiquement le contenu des données EMM_data_byte d'un message EMM d'appariement. Ce contenu dépend de la fonction à exécuter par le décodeur 2 pour la configuration ou l'utilisation de l'appariement.

Les données EMM_data_byte incluent les paramètres fonctionnels suivants :

- ADF 20: complément d'adressage d'un décodeur dans un groupe de décodeurs ; ce paramètre est utile en cas d'adressage par groupe sinon il peut être omis ; il peut être chiffré,
- SOID 22 : identification de messages d'appariement selon l'invention, parmi d'autres types de messages,
- OPID/NID 24 : identification du parc de décodeurs et du signal de l'opérateur,
- TIME 26 : données d'horodatage de l'émission du message ; ce paramètre est utilisé pour éviter le rejeu du message par un même décodeur,

- CRYPTO 28 : identification des fonctions de protection cryptographique appliquées aux paramètres FUNCTIONS 32.

Les paramètres FUNCTIONS peuvent être chiffrés et protégés par une redondance cryptographique 30.

- FUNCTIONS 32 : ensemble des paramètres décrivant la configuration et l'utilisation de l'appariement.

Les paramètres fonctionnels ci-dessus sont organisés librement dans les données EMM_data_byte d'un message EMM. Une implémentation préférée est la combinaison de ces paramètres par structure T L V (Type Longueur Valeur).

TRAITEMENT DES MESSAGES EMM

Les paramètres fonctionnels ci-dessus sont destinés à être traités par le décodeur 2.

Quand ils sont transmis dans un EMM décodeur, ces paramètres constituent le contenu utile de l'EMM.

Quand ils sont transmis dans un EMM carte, ces paramètres constituent une partie, clairement identifiable par la carte, du contenu utile de l'EMM qui contient d'autres paramètres concernant la carte. Cette dernière se charge alors d'extraire les paramètres fonctionnels qui le concernent de l'EMM et de les transmettre au décodeur 2. Une réalisation préférée pour permettre ce mécanisme de tri consiste à intégrer ces paramètres fonctionnels dans un paramètre d'encapsulation non traitable par la carte. Ainsi, à la

détection par la carte 6 de cette encapsulation, la carte 6 envoie au décodeur 2 une réponse de type « Paramètre Non Interprétable (PNI) » accompagnée de l'ensemble des paramètres du décodeur 2.

La carte 6 reçoit également un ordre daté d'inscription de données via un EMM carte, permettant, d'une part, de s'assurer que la carte 6 n'a pas déjà traité ce message dans un autre décodeur, afin d'éviter le rejeu sur un autre décodeur et, d'autre part, de limiter le traitement de cet EMM par un seul décodeur. Sémantiquement ces données signifient « Déjà traité ». Une réalisation préférée de ce mécanisme d'anti-rejeu est l'inscription de ces données d'anti-rejeu dans un bloc de données FAC (Facilities Data Block en anglais) de la carte.

Si suite au traitement d'un EMM_carte d'appariement la carte répond « PNI » et « Déjà Traité» le décodeur 2 ne prend pas en compte les paramètres qu'il reçoit.

CONFIGURATION ET UTILISATION DE L'APPARIEMENT

L'ensemble des paramètres FUNCTIONS 32 décrit la configuration et l'utilisation de l'appariement selon l'invention. Cet ensemble de paramètres est une combinaison quelconque des paramètres fonctionnels suivants :

- MODE : ce paramètre active, désactive ou réinitialise la solution d'appariement. Après désactivation, le décodeur ne contrôle pas l'identifiant d'une carte insérée dans le décodeur mais conserve la liste des identifiants déjà mémorisés, et après réinitialisation, le décodeur ne contrôle pas

l'identifiant d'une carte insérée et n'a plus d'identifiant de cartes mémorisé.

- NBCA (Nombre de cartes autorisées) : ce paramètre impose le nombre maximal d'identifiants de cartes qu'un décodeur est autorisé à mémoriser ; quand il n'est pas renseigné, NBCA est défini par l'implémentation du module logiciel dans le décodeur selon l'invention

- LCA (Liste de cartes autorisées) : ce paramètre impose à un décodeur la liste des identifiants de cartes avec lesquelles il peut fonctionner.

- Perturbation : ce paramètre décrit la perturbation à appliquer par le décodeur dans l'accès aux données en cas de carte non appariée avec le décodeur.

Les paramètres fonctionnels ci-dessus sont organisés librement dans l'ensemble de paramètres FUNCTIONS 32. Une implémentation préférée est la combinaison de ces paramètres par structure T L V (Type Longueur Valeur).

FONCTIONNEMENT

Le fonctionnement de l'appariement selon l'invention va maintenant être décrit par référence aux figures 5 et 6.

La figure 5 est un diagramme fonctionnel illustrant schématiquement les états de la fonction d'appariement du logiciel de contrôle d'accès 4 embarqué dans un décodeur 2.

La fonction d'appariement est dans l'état inactif 60 quand le logiciel de contrôle d'accès 4

vient d'être installé ou téléchargé (étape 61) ou quand il a reçu de la plateforme 1 un ordre de désactivation de l'appariement (étape 62) ou de réinitialisation de l'appariement (étape 64). Dans cet état le logiciel de contrôle d'accès 4 accepte de fonctionner avec une carte 6 insérée dans le décodeur 2 sans vérifier son appariement avec cette carte.

Pour effectuer l'activation de l'appariement dans un décodeur 2, l'opérateur définit via la plateforme 1 un mode d'appariement (= actif), optionnellement le nombre maximum NBCA de cartes 6 susceptibles d'être appariées avec le décodeur 2 et le type de perturbation applicable dans l'accès aux données en cas d'échec de l'appariement. En fonction de ces informations la plateforme 1 génère et émet (flèche 68) un message EMM adressant le ou les décodeurs concernés et contenant les paramètres de configuration. La fonction d'appariement dans le décodeur passe à l'état actif 70.

L'opérateur peut désactiver l'appariement dans le décodeur 2, via la plateforme 1 qui génère et émet (flèche 72) un message EMM adressant le ou les décodeurs concernés et contenant un ordre de désactivation sans effacement du contexte d'appariement 62 ou un ordre de RAZ du contexte d'appariement 64. La fonction d'appariement dans le décodeur passe à l'état inactif 60.

Quel que soit l'état inactif ou actif de la fonction d'appariement, elle peut recevoir (étape 74) une liste de cartes autorisées LCA par EMM émise par la plateforme 1.

La prise en compte d'une carte 6 par la fonction d'appariement dans un décodeur 2 est décrite dans l'organigramme de la figure 6.

A l'insertion (étape 80) d'une carte 6 dans le décodeur 2, le logiciel de contrôle d'accès 4 embarqué dans le décodeur teste (étape 82) si la fonction d'appariement est dans l'état actif 70.

Si la fonction d'appariement dans le décodeur est dans l'état inactif 60, le décodeur accepte de fonctionner avec la carte insérée (étape 92).

Si la fonction d'appariement dans le décodeur est dans l'état actif 70, le logiciel de contrôle d'accès lit l'identifiant de la carte et vérifie (étape 84) si cet identifiant de la carte insérée est déjà mémorisé dans le décodeur 2. Si l'identifiant de cette carte 6 est déjà mémorisé dans le décodeur 2, le logiciel de contrôle d'accès 4 accepte de fonctionner avec la carte insérée (étape 92). Dans ce cas, l'accès aux programmes diffusés est alors possible, sous réserve de conformité des autres conditions d'accès attachées à ces programmes.

Si l'identifiant de cette carte 6 n'est pas mémorisé dans le décodeur 2, le logiciel de contrôle d'accès vérifie (étape 86) si le nombre d'identifiants de cartes 6 déjà mémorisés est inférieur à la valeur maximum NBCA de cartes 6 autorisées par la configuration.

- Si ce nombre NBCA est atteint, le logiciel de contrôle d'accès 4 refuse de fonctionner avec la carte 6 insérée dans le lecteur du décodeur

2, et applique (étape 90) la perturbation dans l'accès aux données telle que définie par l'opérateur. Une telle perturbation peut consister à bloquer l'accès aux programmes diffusés. Elle peut être accompagnée de l'affichage sur l'écran du terminal auquel est associé le décodeur 2 d'un message invitant l'abonné à insérer une autre carte 6 dans le décodeur 2,

- Si ce nombre NBCA n'est pas atteint, l'identifiant de la carte 6 insérée dans le lecteur du décodeur 2 est ajouté à la liste des identifiants mémorisés (étape 88). Le logiciel de contrôle d'accès 4 accepte ensuite de fonctionner avec la carte 6 insérée (étape 92).

Quand la carte 6 est extraite (étape 94) du décodeur 2, le logiciel de contrôle d'accès 4 passe en attente de l'insertion d'une carte 6 (étape 80).

La perturbation 90 dans l'accès aux données en cas de défaut d'appariement peut être de différente nature telle que par exemple :

- Arrêt audio et vidéo sur les chaînes cryptées (obtenu par non soumission des ECM à la carte pour calcul des CW) ;
- Arrêt audio et vidéo sur les chaînes en clair et analogiques (obtenu par message au middleware) ;
- Envoi d'un message au middleware du terminal (exemple : message Open TV).

Cette perturbation peut être utilisée également pour provoquer le blocage de décodeurs volés.

Dans le cas décrit dans la figure 2 où le logiciel de contrôle d'accès 4 est exécuté dans l'interface amovible 8 connectée à un décodeur 2, l'automate décrit dans la figure 4 et l'organigramme décrit dans la figure 5 s'appliquent directement au logiciel de contrôle d'accès embarqué 4 dans cette interface amovible 8.

REVENDICATIONS

1. Procédé d'appariement d'un équipement récepteur de données numériques (2) avec une pluralité de modules externes de sécurité (6, 8) ayant chacun un identifiant unique, procédé caractérisé en ce qu'il comporte les étapes suivantes :

- connecter un module externe de sécurité (6, 8) à l'équipement récepteur,
- mémoriser à la volée dans l'équipement récepteur (2) l'identifiant unique du module de sécurité (6, 8) connecté.

2. Procédé selon la revendication 1, caractérisé en ce qu'il comporte en outre une phase de contrôle consistant à vérifier, à chaque connexion ultérieure d'un module externe de sécurité (6, 8) à l'équipement récepteur(2), si l'identifiant dudit module est mémorisé dans cet équipement récepteur (2).

3. Procédé selon la revendication 2, caractérisé en ce qu'il comporte en outre une étape consistant à transmettre à l'équipement récepteur (2) une signalisation comportant au moins un message de gestion de la mémorisation de l'identifiant du module externe de sécurité (6, 8) et/ou un message de gestion de la phase de contrôle.

4. Procédé selon la revendication 3, caractérisé en ce que ladite signalisation comporte au moins une des consignes suivantes :

- autoriser la mémorisation,
- interdire la mémorisation,
- effacer les identifiants déjà mémorisés dans l'équipement récepteur (2),

- activer ou désactiver la phase de contrôle.

5. Procédé selon la revendication 3, caractérisé en ce que ladite signalisation comporte en outre le nombre maximal d'identifiants dont la mémorisation est autorisée.

6. Procédé selon la revendication 3, caractérisé en ce que ladite signalisation comporte une consigne de reconfiguration par laquelle on transmet à l'équipement récepteur (2) une liste mise à jour des identifiants des modules externes de sécurité (6, 8) appariés avec ledit équipement récepteur (2).

7. Procédé selon la revendication 6, caractérisé en ce que ladite liste est transmise directement à l'équipement récepteur (2).

8. Procédé selon la revendication 6, caractérisé en ce que ladite liste est transmise via un module externe de sécurité (6, 8) connecté audit équipement récepteur (2).

9. Procédé selon la revendication 2, dans lequel ladite phase de contrôle comporte une procédure consistant à perturber le traitement des données si l'identifiant du module externe de sécurité (6, 8) connecté n'est pas préalablement mémorisé l'équipement récepteur (2).

10. Procédé selon la revendication 1, caractérisé en ce que lesdites données sont distribuées en clair ou embrouillées par un mot de contrôle chiffré, et en ce que chaque module externe de sécurité (6, 8) comporte des droits d'accès auxdites données et un algorithme de déchiffrement dudit mot de contrôle .

11. Procédé selon l'une des revendications 4 ou 5, caractérisé en ce que ladite signalisation est transmise à un équipement récepteur (2) dans un message EMM spécifique à un module externe de sécurité (6, 8) associé à cet équipement récepteur (2).

12. Procédé selon l'une des revendications 4 ou 5, caractérisé en ce que ladite signalisation est transmise à un équipement récepteur (2) dans un message EMM spécifique à cet équipement récepteur (2).

13. Procédé selon la revendication 6, caractérisé en ce que, pour un équipement récepteur (2) donné, ladite liste est transmise dans un message EMM spécifique à un module de sécurité (6, 8) associé à cet équipement récepteur (2).

14. Procédé selon l'une des revendications 4 ou 5, caractérisé en ce que ladite signalisation est transmise à un groupe d'équipements récepteurs (2) dans un message EMM spécifique à un groupe de modules externes de sécurité (6, 8) associés auxdits équipements récepteurs (2).

15. Procédé selon l'une des revendications 4 ou 5, caractérisé en ce que ladite signalisation est transmise à un groupe d'équipements récepteurs (2) dans un message EMM spécifique audit groupe d'équipements récepteurs (2).

16. Procédé selon la revendication 6, caractérisé en ce que, pour un groupe d'équipements récepteurs (2) donné, ladite liste est transmise dans un message EMM spécifique à un groupe de modules externes de sécurité (6, 8) associées auxdits équipements récepteurs (2).

17. Procédé selon l'une des revendications 4 ou 5, caractérisé en ce que ladite signalisation de contrôle est transmise dans un flux privé à un groupe d'équipements récepteurs (2).

18. Procédé selon la revendication 6, caractérisé en ce que, pour un groupe d'équipements récepteurs (2) donné, ladite liste est transmise dans un flux privé à chaque équipement récepteur (2).

19. Procédé selon l'une des revendications 17 ou 18, caractérisé en ce que ledit flux privé est traité par un logiciel dédié exécutable dans chaque équipement récepteur (2) en fonction de l'identifiant du module externe de sécurité (6, 8) qui lui est associé.

20. Procédé selon l'une des revendications 11 à 16, caractérisé en ce qu'il comporte en outre un mécanisme destiné empêcher l'utilisation d'un EMM transmis à un même module externe de sécurité (6, 8) dans deux équipements récepteurs (2) distincts.

21. Procédé selon l'une des revendications 11 à 13, caractérisé en ce que ledit EMM présente le format suivant :

```
EMM-U_section() {
table_id = 0x88                          8 bits
section_syntax_indicator = 0             1 bit
DVB_reserved                             1 bit
ISO_reserved                             2 bits
EMM-U_section_length                     12 bits
unique_adress_field                      40 bits
for (i=0; i<N; i++) {
    EMM_data_byte                        8 bits
    }
}
```

22. Procédé selon l'une des revendications 14 à 16, caractérisé en ce que ledit EMM est spécifique à tous les modules externes de sécurité (6, 8) ou à tous les équipements récepteurs (2) et présente le format suivant :

```
EMM-G_section() {
table_id = 0x8A ou 0x8B                 8 bits
section_syntax_indicator = 0            1 bit
DVB_reserved                            1 bit
ISO_reserved                            2 bits
EMM-G_section_length                    12 bits
for (i=0; i<N; i++) {
    EMM_data_byte                       8 bits
    }
}
```

23. Procédé selon l'une des revendications 14 à 16, caractérisé en ce que ledit EMM est spécifique à un sous-groupe de modules externes de sécurité (6, 8) ou d'équipements récepteurs (2) et présente le format suivant :

```
EMM-S_section() {
table_id = 0x8E                         8 bits
section_syntax_indicator = 0            1 bit
DVB_reserved                            1 bit
ISO_reserved                            2 bits
EMM-S_section_length                    12 bits
shared_address_field                    24 bits
reserved                                6 bits
data_format                             1 bit
ADF_scrambling_flag                     1 bit
for (i=0; i<N; i++) {
    EMM_data_byte                       8 bits
    }
}
```

24. Procédé selon la revendication 1, caractérisé en ce que les identifiants de modules externe de sécurité (6, 8) sont groupés dans une liste chiffrée.

25. Procédé selon l'une quelconque des revendications 1 à 24, caractérisé en ce que l'équipement récepteur (2) comporte un décodeur et le module externe de sécurité (6, 8) comporte une carte de contrôle d'accès (6) dans laquelle sont mémorisées des informations relatives aux droits d'accès d'un abonné à des données numériques distribuées par un opérateur, et en ce que l'appariement est effectué entre ledit décodeur et ladite carte (6).

26. Procédé selon l'une quelconque des revendications 1 à 24, caractérisé en ce que l'équipement récepteur (2) comporte un décodeur et le module externe de sécurité (6, 8) comporte une interface de sécurité amovible (8) munie d'une mémoire non volatile et destinée à coopérer, d'une part, avec le décodeur, et d'autre part, avec une pluralité de cartes de contrôle (6) d'accès conditionnel pour gérer l'accès à des données numériques distribuées par un opérateur, et en ce que l'appariement est effectué entre ledit décodeur et ladite interface (8) de sécurité amovible.

27. Procédé selon l'une quelconque des revendications 1 à 24, caractérisé en ce que l'équipement récepteur (2) comporte un décodeur muni d'une interface de sécurité amovible (8) ayant une mémoire non volatile et destinée à coopérer, d'une part, avec ledit décodeur, et d'autre part, avec une

pluralité de cartes de contrôle (6) d'accès conditionnel et en ce que l'appariement est réalisé entre ladite interface de sécurité amovible (8) et lesdites cartes de contrôle d'accès (6).

28. Procédé selon la revendication 10, caractérisée en ce que les données sont des programmes audiovisuels.

29. Equipement récepteur (2) susceptible d'être apparié avec une pluralité de modules externes de sécurité (6, 8) pour gérer l'accès à des données numériques distribuées par un opérateur, caractérisé en ce qu'il comporte des moyens pour mémoriser à la volée l'identifiant de chaque module externe de sécurité (6, 8) qui lui est connecté.

30. Equipement selon la revendication 29, caractérisé en ce qu'il comporte un décodeur et en ce que le module externe de sécurité (6, 8) est une carte de contrôle d'accès (6) comportant des informations relatives aux droits d'accès d'un abonné auxdites données numériques, l'appariement étant effectué entre ledit décodeur et ladite carte (6).

31. Equipement selon la revendication 29, caractérisé en ce qu'il comporte un décodeur et en ce que le module externe de sécurité (6, 8) est une interface de sécurité amovible (8) munie d'une mémoire non volatile et destinée à coopérer, d'une part, avec ledit décodeur, et d'autre part, avec une pluralité de cartes de contrôle d'accès conditionnel (6), pour gérer l'accès auxdites données numériques, l'appariement étant effectué entre ledit décodeur et ladite interface de sécurité amovible (8).

32. Equipement selon la revendication 29, caractérisé en ce qu'il comporte un décodeur muni d'une interface de sécurité amovible (8) ayant une mémoire non volatile et destinée à coopérer, d'une part, avec ledit décodeur, et d'autre part, avec une pluralité de cartes de contrôle (6) d'accès conditionnel et en ce que l'appariement est réalisé entre ladite interface de sécurité amovible (8) et lesdites cartes de contrôle d'accès (6).

33. Décodeur susceptible de coopérer avec une pluralité de modules externes de sécurité (6, 8) pour gérer l'accès à des programmes audiovisuels distribués par un opérateur, chaque module externe de sécurité (6, 8) ayant un identifiant unique et comportant au moins un algorithme de traitement de données, décodeur caractérisé en ce qu'il comporte des moyens pour mémoriser à la volée l'identifiant de chaque module externe de sécurité (6, 8) qui lui est connecté.

34. Décodeur selon la revendication 33, caractérisé en ce que lesdits modules externes de sécurité (6, 8) sont des cartes de contrôle d'accès (6) dans lesquelles sont mémorisées des informations relatives aux droits d'accès d'un abonné à des données numériques distribuées par un opérateur .

35. Décodeur selon la revendication 33, caractérisé en ce que lesdits modules externes de sécurité (6, 8) sont des interfaces de sécurité amovibles (8) comportant une mémoire non volatile et destinées à coopérer, d'une part, avec le décodeur, et d'autre part, avec une pluralité de cartes de contrôle

d'accès (6) conditionnel pour gérer l'accès à des données numériques distribuées par un opérateur.

36. Interface de sécurité amovible (8) comportant une mémoire non volatile et destinée à coopérer, d'une part, avec un équipement récepteur (2), et d'autre part, avec une pluralité de cartes de contrôle d'accès (6) conditionnel, pour gérer l'accès à des données numériques distribuées par un opérateur, chaque carte (6) ayant un identifiant unique et comportant des informations relatives aux droits d'accès d'un abonné auxdites données numériques, interface caractérisée en ce qu'elle comporte des moyens pour enregistrer à la volée l'identifiant de chaque carte de contrôle d'accès (6) dans ladite mémoire non volatile.

37. Interface selon la revendication 36 caractérisée en ce qu'elle consiste en une carte PCMCIA comportant un logiciel de désembrouillage de données numériques.

38. Interface selon la revendication 36 caractérisée en ce qu'elle consiste en un module logiciel.

39. Programme d'ordinateur exécutable dans un équipement récepteur (2) susceptible de coopérer avec une pluralité de modules externes de sécurité (6, 8) ayant chacun un identifiant unique et dans lesquels sont stockées des informations relatives aux droits d'accès d'un abonné à des données numériques distribuées par un opérateur, caractérisé en ce qu'il comporte des instructions pour mémoriser à la volée

l'identifiant de chaque module externe de sécurité (6, 8) connecté audit équipement récepteur (2).

40. Programme d'ordinateur selon la revendication 39, caractérisé en ce qu'il comporte en outre des instructions destinées à générer localement des paramètres de contrôle de l'appariement de l'équipement récepteur (2) avec un module externe de sécurité (6, 8) en fonction d'une signalisation transmise audit équipement récepteur (2) par l'opérateur.

41. Programme d'ordinateur selon la revendication 39, caractérisé en ce qu'il comporte en outre des instructions destinées à vérifier, à chaque utilisation ultérieure d'un module externe de sécurité (6, 8) avec l'équipement récepteur (2), si l'identifiant dudit module externe de sécurité (6, 8) est mémorisé dans l'équipement récepteur (2).

42. Système comportant une pluralité d'équipements récepteurs (2) connectés à un réseau de diffusion de données et/ou services, chaque équipement récepteur (2) étant susceptible d'être apparié avec une pluralité de modules externes de sécurité (6, 8), ledit système comportant également une plateforme de gestion commerciale (1) communiquant avec les équipements récepteurs (2) et avec lesdits modules externes de sécurité (6, 8), caractérisé en ce qu'il comporte en outre :

- un premier module agencé dans ladite plate-forme de gestion commerciale (1) et destiné à générer des requêtes d'appariement,

- et un deuxième module agencé dans lesdits équipements récepteurs (2) et destiné à traiter lesdites requêtes pour préparer une configuration de l'appariement et pour contrôler l'appariement.

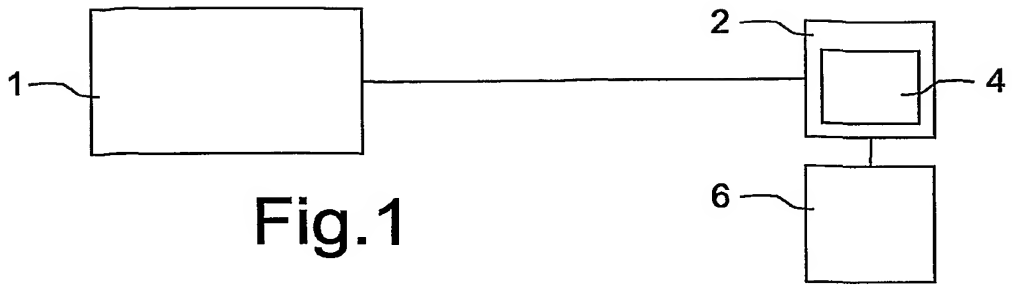


Fig.1

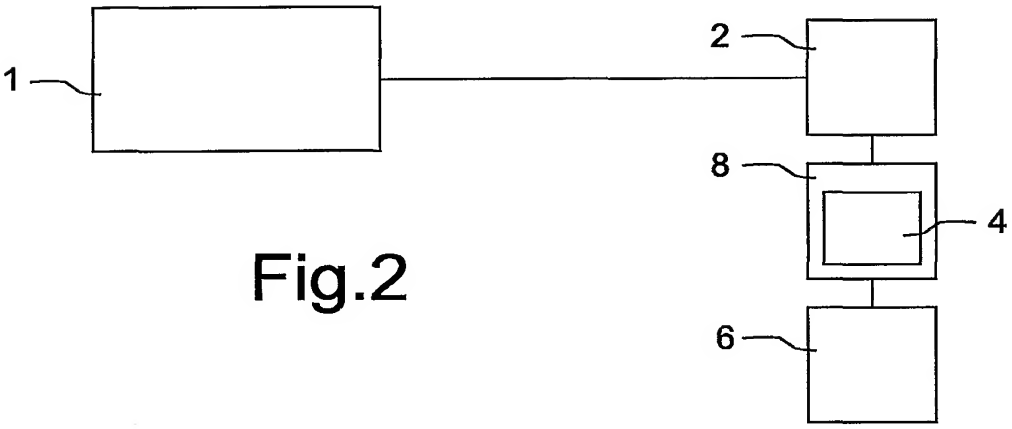


Fig.2

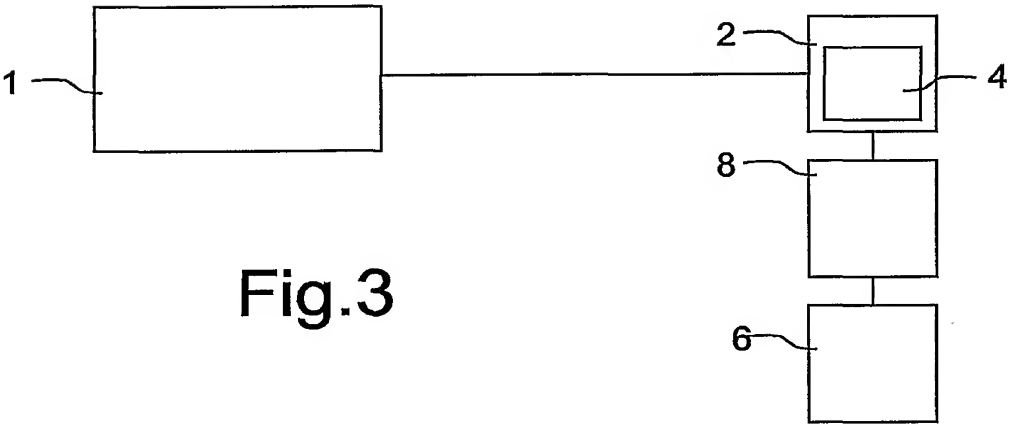


Fig.3

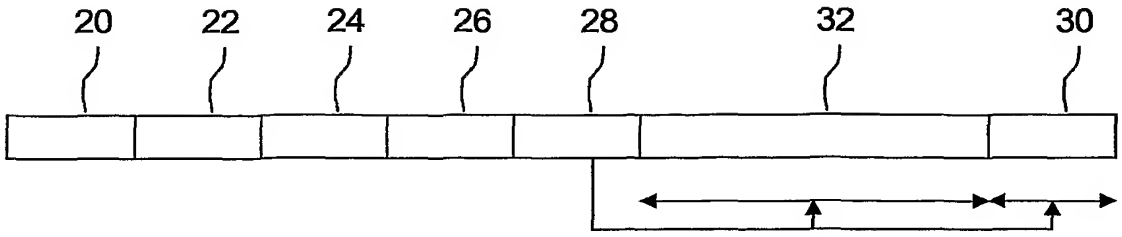


Fig.4

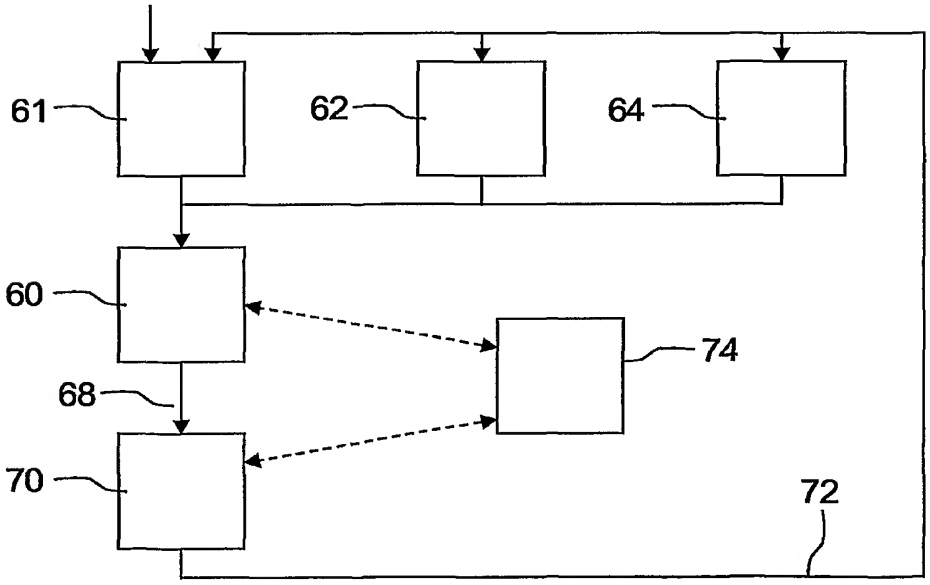


Fig.5

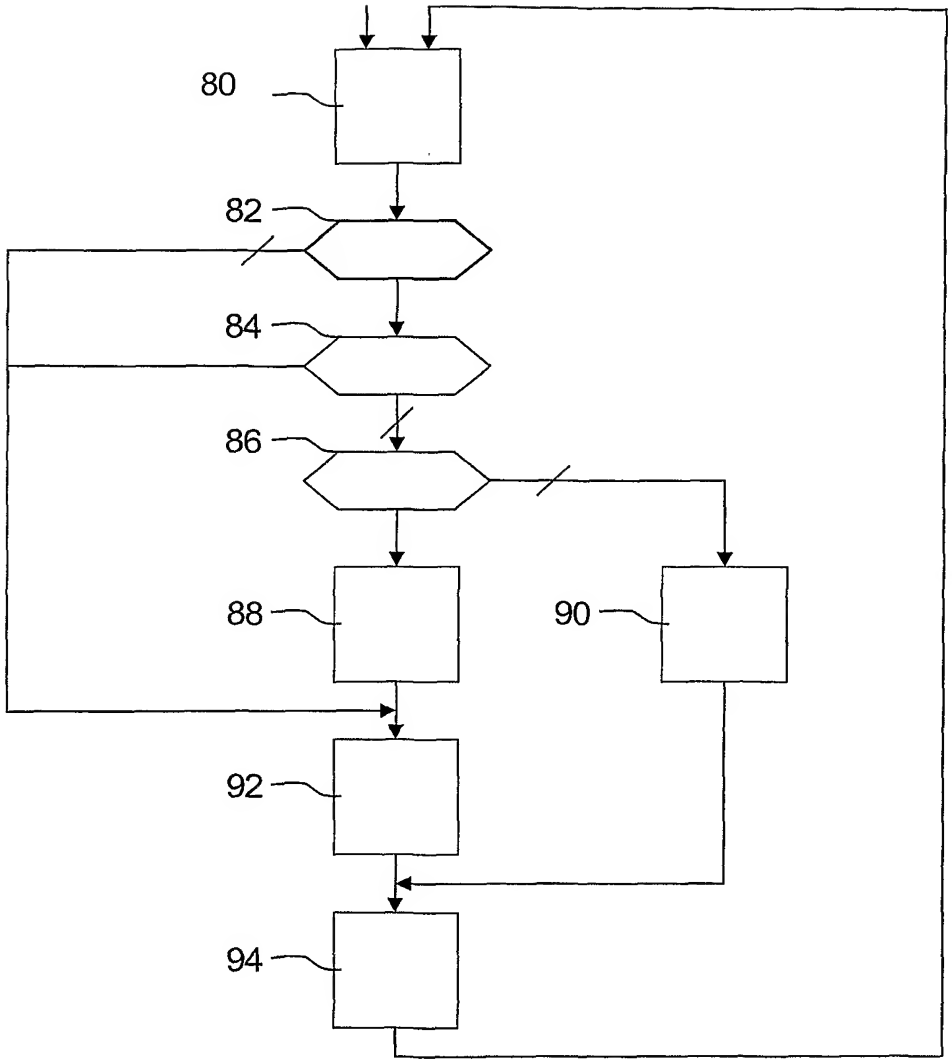


Fig.6

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR2005/050101

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/167 H04N5/00 H04N7/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 99/57901 A (KUDELSKI SA ; KUDELSKI ANDRE (CH); SASSELLI MARCO (CH)) 11 November 1999 (1999-11-11) cited in the application the whole document claims 2,4	1-42
A	KANJANARIN W ET AL: "Scrambling and key distribution scheme for digital television" ., 10 October 2001 (2001-10-10), pages 140-145, XP010565513 paragraphs '0001!, '0004!	1-42

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 June 2005	29/06/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Schneiderlin, J

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR2005/050101

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO 9957901 A	11-11-1999	AT	222441 T	15-08-2002
		AU	751436 B2	15-08-2002
		AU	3529799 A	23-11-1999
		BG	64137 B1	30-01-2004
		BG	104905 A	29-06-2001
		BR	9909710 A	26-12-2000
		CN	1314047 A ,C	19-09-2001
		DE	69902527 D1	19-09-2002
		DE	69902527 T2	08-05-2003
		DK	1078524 T3	25-11-2002
		EA	2703 B1	29-08-2002
		EE	200000639 A	15-04-2002
		EP	1078524 A1	28-02-2001
		ES	2181418 T3	16-02-2003
		HR	20000753 A1	31-10-2001
		HU	0301133 A2	28-08-2003
		WO	9957901 A1	11-11-1999
		ID	26103 A	23-11-2000
		JP	2002514862 T	21-05-2002
		NO	20005533 A	02-11-2000
		NZ	507807 A	26-11-2002
		PL	343941 A1	10-09-2001
		PT	1078524 T	31-12-2002
		SI	1078524 T1	31-12-2002
		SK	16492000 A3	10-05-2001
		TR	200003258 T2	21-03-2001
		TW	412909 B	21-11-2000
		ZA	200006172 A	14-05-2001

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR2005/050101

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04N7/167 H04N5/00 H04N7/16

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04N

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 99/57901 A (KUDELSKI SA ; KUDELSKI ANDRE (CH); SASSELLI MARCO (CH)) 11 novembre 1999 (1999-11-11) cité dans la demande le document en entier revendications 2,4	1-42
A	KANJANARIN W ET AL: "Scrambling and key distribution scheme for digital television" ., 10 octobre 2001 (2001-10-10), pages 140-145, XP010565513 alinéas '0001!, '0004!	1-42

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
15 juin 2005	29/06/2005

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Schneiderlin, J

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande Internationale No
PCT/FR2005/050101

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 9957901 A	11-11-1999	AT 222441 T	15-08-2002
		AU 751436 B2	15-08-2002
		AU 3529799 A	23-11-1999
		BG 64137 B1	30-01-2004
		BG 104905 A	29-06-2001
		BR 9909710 A	26-12-2000
		CN 1314047 A ,C	19-09-2001
		DE 69902527 D1	19-09-2002
		DE 69902527 T2	08-05-2003
		DK 1078524 T3	25-11-2002
		EA 2703 B1	29-08-2002
		EE 200000639 A	15-04-2002
		EP 1078524 A1	28-02-2001
		ES 2181418 T3	16-02-2003
		HR 20000753 A1	31-10-2001
		HU 0301133 A2	28-08-2003
		WO 9957901 A1	11-11-1999
		ID 26103 A	23-11-2000
		JP 2002514862 T	21-05-2002
		NO 20005533 A	02-11-2000
		NZ 507807 A	26-11-2002
		PL 343941 A1	10-09-2001
		PT 1078524 T	31-12-2002
		SI 1078524 T1	31-12-2002
		SK 16492000 A3	10-05-2001
		TR 200003258 T2	21-03-2001
		TW 412909 B	21-11-2000
		ZA 200006172 A	14-05-2001